Enabling Geospatial Context in an IoT Decentralised Reputation Management System using Ethereum Smart Contracts

Ponlawat Weerapanpisit, Sergio Trilles, Joaquín Huerta
Institute of New Imaging Technologies (INIT)
Universitat Jaume I
Castell´o de la Plana, Spain
al394260, strilles, huerta@uji.es

Marco Painho
NOVA IMS
Universidade
Nova de Lisboa
Lisboa, Portugal
painho@novaims.
unl.pt

This is the accepted version of the conference paper published by IEEE at *2021 IEEE International Conference on Omni-Layer Intelligent Systems, COINS 2021:*

How to cite: Weerapanpisit, P., Trilles, S., Huerta, J., & Painho, M. (2021). Enabling geospatial context in an iot decentralised reputation management system using ethereum smart contracts. In 2021 IEEE International Conference on Omni-Layer Intelligent Systems, COINS 2021 (pp. 1-6). (2021 IEEE International Conference on Omni-Layer Intelligent Systems, COINS 2021). Institute of Electrical and Electronics Engineers Inc.. https://doi.org/10.1109/COINS51742.2021.9524217

Enabling Geospatial Context in an IoT Decentralised Reputation Management System using Ethereum Smart Contracts

Ponlawat Weerapanpisit, Sergio Trilles, Joaquín Huerta
Institute of New Imaging Technologies (INIT)
Universitat Jaume I
Castelló de la Plana, Spain
al394260, strilles, huerta@uji.es

Marco Painho
NOVA IMS
Universidade Nova de Lisboa
Lisboa, Portugal
painho@novaims.unl.pt

***Abstract*—Social Internet of Things (SIoT) is a concept that integrates the Internet of Things and human social networks. An SIoT system has to store and manage device reputation values, which are used by end devices to determine the trustworthiness of another one. This device trustworthiness can also be affected by its geographical location. In this work, we introduced an architecture that includes the geospatial context in the part concerned with reputation management. The proposed architecture is based on the cloud-fog-edge architecture and uses the fog layer as the management system. The devices in the fog layer form an Ethereum Blockchain network and store the Smart Contracts. These in turn allow the management functionalities to be carried out in a decentralised, transparent and secure way, which are the advantages of Blockchain. To enable the characteristics with a geospatial component, it is necessary to apply a geocoding technique. This work shows how geocoding techniques can be adapted to cover the main geospatial functionalities and compares two geocoding options (Geohash or S2). The results showed that it is possible to include the geospatial context in a decentralised reputation management system by using hierarchical geocoding techniques, and the experiments showed that both Geohash and S2 can offer a similar performance in the proposed architecture.**

***Index Terms*—Internet of Things, Reputation Management, Geocoding, Blockchain**

I. Introduction

Since the beginning of the Internet of Things (IoT), the number of IoT devices has grown steadily [1], [2]. Thanks to the development of communication technologies, a larger number of devices can connect to the internet network and communicate with each other to exchange their data and information. However, this leads to a consequent issue of trustworthiness. Consuming a service from an untrustworthy IoT device can affect the system functionality and cause an unexpected failure [3], [4]. An IoT system therefore needs to be able to manage trust between devices.

This study was supported by the TRUST4IoE project of the Programa Estatal de Proyectos de I+D de Generación de Conocimiento of the Spanish government (grant number PID2019-104065GA-I00). Sergio Trilles has been funded by the postdoctoral Juan de la Cierva fellowship programme of the Spanish Ministry for Science and Innovation (IJC2018-035017-I). 978-1-6654-3156-9/21/$31.00 ©2021 IEEE

The trustworthiness of a device towards another one can be derived from different factors. It can be based on a reputation value, which can be calculated from device behaviour in the past, such as the quality of the data that it produced [4]. The trustworthiness of a device can also be affected by the location of the device in space [5]. Because IoT devices can be moved from and to different places, their geographical location can affect their trustworthiness. For this reason, in order to manage trust in an IoT system, the management system should also include the geospatial context.

Blockchain is a technology that allows data in a network to be stored in a system in a distributed and decentralised way. Due to the asymmetric encryption algorithms that Blockchain uses to validate the transactions, the data in the system, despite being public and accessible to anyone, cannot be altered by another party once they have been published by a valid owner. This property makes Blockchain transparent, secure, and fault-tolerant [6]. Given the characteristics of the IoT, where multiple devices are distributed and connected via the internet, Blockchain can be adopted and implemented in an IoT system to serve various proposes, including the management of trust. Consequently, the reputation management system of an IoT system using Blockchain guarantees the transparency, security and decentralisation properties, which are the main advantages of Blockchain.

Spatial data handling in a computer system can be troublesome as the data are multidimensional and generally related to coordinate systems. Geometric mathematical formulas are needed to calculate and manipulate the data, which leads to more complex algorithms in the computer [21]. Geocoding, which is a methodology for converting a geographical feature into another format, can be used to ease the problem. Some geocoding techniques, for instance, Geohash or Google S2, encode a geolocation into a hierarchical binary-based representation, which is easier to calculate in a computer system because the data notation is binary based [12]. Despite some tolerable loss of precision by these techniques, geocoding can be used to determine the geospatial context in the Blockchain of the reputation management system.

In this context, this work introduces how we can integrate the geospatial dimension into an IoT decentralised reputation management system by using the geographical location of the end devices to determine their reputation values. The management system will be decentralised in the fog layer of the architecture, by making each device in the layer to be an Ethereum Blockchain node and to serve the Smart Contracts for interacting with other layers. Finally, this study shows two experiments conducted to compare two geocoding techniques, Geohash and S2, in the proposed system.

II. Background

A. Trust and Reputation

Social Internet of Things (SIoT) is considered an integration between IoT and human social networks. Atzori et al. proposed the idea of SIoT, where end devices can discover each other and establish a new connection to consume services in the same way as humans do [7]. Figure 1 shows a comparison of the components in a human social network and the Social Internet of Things. According to their proposed framework, relationship management in a human social network is equivalent to the trustworthiness management system in SIoT. A node uses this reputation value as a factor to decide whether it will trust the other node or not before starting the relationship [8].

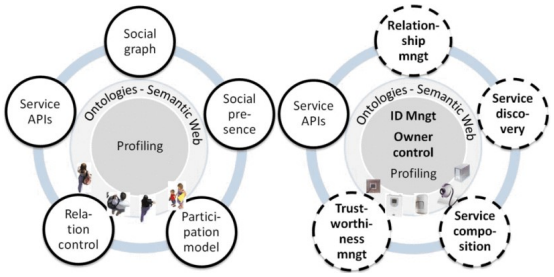

Fig. 1. Atzori et al.'s work [7], the components of human social networks (left) and machines or SIoT (right)

B. Cloud-Fog-Edge Architecture

Due to the progressive development and application of IoT, an IoT system could grow and contain a huge number of devices. This could cause a huge workload in terms of data storage and processing in the cloud device. Consequently, Cisco proposed the cloud-fog-edge layered architecture for the IoT [9]. This architecture adds a new intermediate layer called the fog layer between the cloud and the edge layer. Unlike cloud devices, fog devices are generally cheaper, but smaller in size and have lower performance. However, they are still smart enough, compared to the edge devices, to be able to perform more complex calculations and be in charge as an intermediate node between the cloud and the edge layer [10].

C. Blockchain and Ethereum Smart Contract

Blockchain is a technology for decentralising data storage in the computer. It was originally invented by Nakamoto S. for storing the monetary transactions and movements of their currency called Bitcoin [11]. Inside a Blockchain network, there are several blocks storing the data, which are money transactions in the case of Bitcoin. These blocks are linked to each other chronologically like a chain. It uses an asymmetric encryption algorithm to create and verify signatures of the transactions and blocks. This guarantees that the data inside a Blockchain network, despite being public and accessible to anyone, will be secure and transparent. The blocks and the chain are stored and synchronised by different nodes in the network. In other words, all nodes contain the same data and are constantly updated when there are changes. However, there might be a problem when different nodes are trying to push a new block at the same time. To tackle this issue, Blockchain uses consensus algorithms to reach a consensus between different nodes in the network in order to agree on the current valid state of the network. To accomplish the consensus, the network needs to have a mechanism of selecting a node that is able to push a new block in the chain. The Proof-of-Work is one of a protocol to do so. It is the most famous as it is adopted by Bitcoin and Ethereum. It gives the right to push a block to the node that can first solve a mathematical problem. Examples of other mechanisms are Proof-of-Stake or Proof-of-Authority.

Ethereum is an implementation of Blockchain technology. Similar to Bitcoin, Ethereum also has its own currency, which is called Ether. The main difference between Ethereum and the other implementations is that, besides transaction data, Ethereum also allows executable programming operations in its block data. The executable programme in Ethereum Blockchain is called Smart Contract. Like a traditional computer program, a Smart Contract can be called for execution and contains its variable states inside the Blockchain network. In consequence, Smart Contracts allow their application to have the advantages that the Blockchain also has, which are transparency, security and being fault-tolerance.

D. Geocoding

Geocoding is a technique used to convert a geospatial feature into another representation. For example, a point on the Earth can be represented in the form of coordinates, a place name or a postal address. The geocoded information is expected to be easier and more understandable for interpreting the feature, even though it is not able to revert the geocoded information to the original feature. Geohash and S2 are geocoding techniques that make the geocoded information hierarchical, binary-oriented and easier for a machine to interpret and calculate. The geocoded information of both techniques represents a cell or an area in space. The two techniques use different algorithms to encode and decode data, and their geocoded information also has different representation structures. However, despite these differences, both of them share the common property of being hierarchical. From these properties, the length of the geocoded information from both techniques can indicate the size of the area or the precision of the target cell. Furthermore, a pair of geocoded cells that have

a mutual prefix also indicate that they are located in the same cell of the upper level. Because of this mutuality, they are adopted to be used in the Smart Contracts for comparison in this work. Figure 2 shows a brief example that demonstrates the hierarchical and the mutual-prefix properties of the two geocoding techniques.

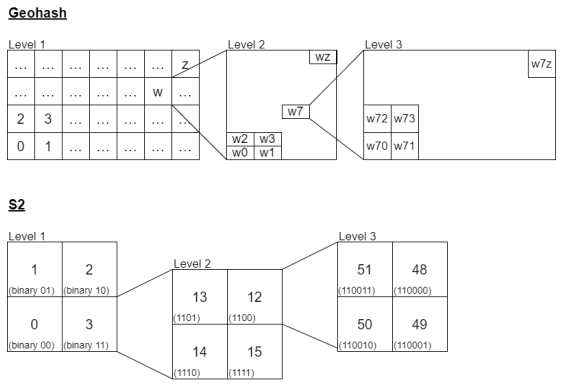

Fig. 2. Hierarchical Geocoding Techniques: Geohash and S2

Geohash is a hierarchical geocoding technique. Its binary data contain the latitude value using those bits in the even positions, and contain the longitude value using those in the odd positions [12]. Geohash data usually use base32 representation to display the binary data, by grouping the binaries into 5 bits per group and assigning a character to represent the value of each group. S2 is another hierarchical geocoding technique and uses the Hillbert space-filling curve to determine the geocoded cell in space [13]. Unlike Geohash, the representation of an S2 cell is usually a decimal or hexadecimal numeric display.

III. Related Works

Several studies have been conducted on the subject of trust and reputation management architecture in an IoT system. Chen et al. proposed an architecture for managing reputation by dividing it into five layers: reputation management layer, organisation layer, Software-Defined Networking (SDN) control layer, node layer and object layer [14]. The organisation layer communicates with users and the reputation management layer handles their requests. This last layer uses the reputation value to decide on trust for the users. Guo et al. proposed a use case scenario of managing trust in an IoT system [15]. Their scenario is a system where devices with sensors share air quality data. In their work, all the trust values between each pair of devices are stored and handled in the cloud layer, which is a centralised approach. Kouicem et al. took a decentralised approach by using Blockchain to manage the trust values between devices in the system [16]. Debe et al. also used Blockchain with Ethereum Smart Contract to create a decentralised application for managing reputation values of fog nodes [17]. However, the geospatial context of the devices was not included in managing their reputation values in these studies.

Besides trust and reputation management in IoT, some research has also demonstrated the possibility of adopting Blockchain technology in an IoT system. Huh et al. used Ethereum Smart Contract to manage and control the behaviour policies of devices in the system [18]. Fernando et al. used Raspberry Pi as a node in Blockchain to store and synchronise the data in the chain of the network [19]. These studies demonstrate that, despite the smaller size and lower computation capability of an IoT device, a number of IoT device variations have enough potential to perform as a Blockchain node.

As the topic is relatively new, no reports of research using geocoding techniques in Blockchain with IoT devices were found. Yet, some authors have studied and compared different geocoding techniques. Deiotte and Valley compared the computational efficiency and utility between raw geographical objects or coordinates, Z-Order space-filling curves or Geohash, and Hilbert space-filling curve or S2 [20]. Their results showed that geocoding based on the Hilbert curve performs better in many aspects. Victor and Zickau implemented the Ethereum Blockchain network and used Geohash and S2 to store geofencing data in Smart Contracts [13]. Their work demonstrated the feasibility of manipulating geospatial data in a decentralised application. And from their study, they concluded that S2 offers better performance than Geohash.

IV. Methodology

This section introduces an architecture of an IoT system for managing device reputation values in a decentralised way. Figure 3 shows the overall structure of the proposed architecture. As it is based on the cloud-fog-edge architecture, the actors are hierarchically divided into three layers: cloud, fog and edge. In the edge layers, there are two roles of the devices, which are those of service provider and service consumer.

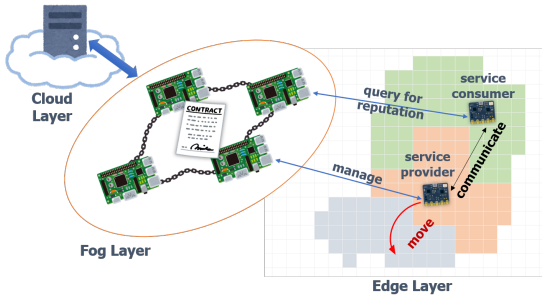

Fig. 3. Overview of the proposed architecture

The first layer is the cloud layer. In general, cloud devices are in charge of upper-level data storage, calculation and analysis. Nevertheless, since the current work focuses on reputation management, which is located in the fog layer, the cloud layer will be of less importance.

The fog layer contains devices that are distributed. The devices in this layer connect and form a Blockchain network. The Blockchain runs Ethereum Smart Contracts to manage the assigned geographical area and the reputation values of edge device services. Fog devices offer an API to serve as an interface between clients from other layers and the Smart Contracts. The Smart Contracts in the fog layer also contain

the spatial data of the geographical regions registered in the system. A region is determined by a list of geocoded cells as shown in Figure 3. Due to the encryption algorithms and use of signatures in the Blockchain, a geographical region registered in the Smart Contracts can be read its data publicly, although it can only be modified from the node that owns the region.

The last layer is the edge layer. This layer contains edge devices that are separated into two roles: service provider and service consumer. The service providers are equipped with sensors to measure data and provide the service when acquired. On the other hand, the service consumers, which are equipped with actuators, consume the service in order to read sensory data from the providers with the aim of acting upon the actuators. The consumers communicate with the fog layer to discover a reputed device that provides the requested service in a geographical area. The service providers can be moved geographically between different areas, and in such cases, their reputation values should be changed.

Every interaction must be carried out through the Fog API. After the system has been deployed, all the geographical regions must be registered in the Smart Contracts by giving the region data and their geocoded cells to each equivalent fog node. The Smart Contracts also exhibit functions that allow the clients to query for the corresponding region by giving a geocoded cell. This function can be called from any node in the fog layer as the data are synchronised through Blockchain. In the same way, the service providers in the edge layer must also register themselves in Smart Contracts so that their services can be discovered by the consumers. The Smart Contracts store the information of the service providers, such as their IP address, geographical location and services being served. Even though the service provider itself is not a Blockchain node, and has to communicate with the Smart Contracts through a fog node, the data and the transactions that belong to the edge device have to be signed before being submitted to the Smart Contracts. In this way, the data submitted by the edge device in the Smart Contracts cannot be modified without knowing the private key, nor can it be modified by the fog node, which is the go-between in the communication.

When a service consumer in the edge layer wants to consume a service, it communicates with a fog node through its API to discover a reputed provider. After the request, the fog node returns a list of available providers and their reputation values in the desired area. The consumer can use this information to select the best candidate that it trusts before directly starting to consume the service with that provider.

Finally, after consuming the service, the fog node receives the data quality from the provider, as well as the service feedback from the consumer. The fog node can use this information to calculate a new reputation value for the provider, before updating it in the Smart Contracts. However, as this work does not focus on generating the reputation values, but on the management system, this calculation part will be presented in another study and will calculate the reputation value based on the data quality and the feedback.

The geospatial data in the Smart Contracts, either the regions that determine device reputation values or the device locations, will be geocoded using the aforementioned hierarchical geocoding techniques: Geohash or S2. The aim of this is to reduce the computational complexity of the programming in the Smart Contracts. Both the techniques are hierarchical but different in terms of their encoding algorithms and their representation. Therefore, they can share most of the Smart Contract methods and inherit the same abstract contract called *Regions*. At the same time, they also override the *query* method, which is the only function that has a different behaviour, because *Geohash* uses 5 bits to represent one level, while S2 uses 2 bits.

Figure 4 shows an example of the geocoded regions. The left image shows the original polygon of the region. The data stored in the Smart Contract will be a set of geocoded cells shown in the right image. Because of this, the binary representation of the geocoding techniques that have been adopted is hierarchical, it can merge the group of cells which fulfil the lower level into one cell in the upper level. This behaviour can be observed in the image on the right of Figure 4.

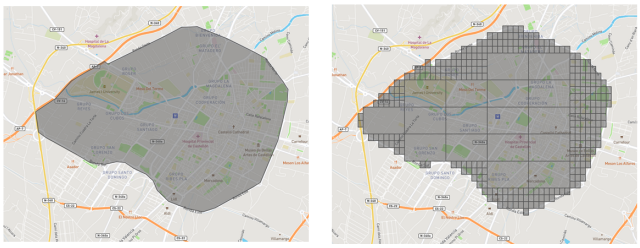

Fig. 4. Example of a polygon covered by geocoded cells

The reputation management system was developed following the proposed architecture. Firstly, the Smart Contracts in the Ethereum Blockchain Network were developed using the Solidity language. The contracts are further split into three different contracts, which are the Regions Contract, Devices Contract and *ReputationManagement* Contract. Figure 5 shows a diagram of the relationship between each pair of contracts.

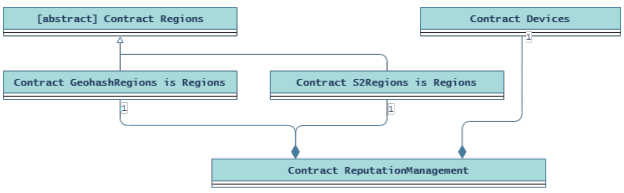

Fig. 5. Relationship Diagram of the Smart Contracts

The *Regions* contract is an abstract contract that is inherited by the other two contracts, depending on the geocoding techniques. The contract contains methods to manage the geographical regions and the geocoded cells data in the system. It also contains a method for finding the corresponding region by giving a geocoded cell ID. Despite the different encoding

algorithms used in Geohash and S2, the geocoded information from both techniques puts binary data in the hierarchical order and, for this reason, the two techniques can share most of the data manipulating methods, and override only the query method, which works differently depending on the technique. The second contract is the *Devices* contract. This contract stores the services and information about devices in the edge layer. It also provides methods that allow the devices to register and update the data by themselves. The last contract is the *ReputationManagement* contract, which joins the Regions and the Devices contracts. It stores the reputation values of device services in different regions. It also contains the methods that allow the clients to discover the desired service and its reputation values.

This work defines two experiments designed to demonstrate that the geospatial component can be included in the Smart Contracts, as well as to compare the two techniques. The first experiment is to compare both geocoding techniques outside the Smart Contracts by encoding a set of polygons and measuring the size of the output file. The second experiment is to compare the energy consumption of handling geocoded data in the Smart Contracts by measuring the Ethereum Gas used to add the data and measuring the time spent on querying for a geocoded cell in the Smart Contracts.

V. Results

The first experiment was performed by encoding the polygon data for the administrative regions in Spain. It compares Geohash precision levels 4, 5, 6 and 7, and S2 precision levels 9, 12, 14 and 17, respectively. Figure 6 shows the resulting file size of the experiment output. From the figure, it can be observed that in the lower level (bigger cell area), S2 requires a larger file size than Geohash, while the opposite occurs in the upper level (smaller cell area). However, this could be affected by the characteristics of the polygons. Because the two techniques have different algorithms for encoding, some polygons might be covered more sufficiently by one technique than with the other. The second reason could be the representation of each technique, as Geohash uses Base32 encoding while S2 uses 64-bit integer to represents one cell. However, there is no clear evidence that one technique gives a better result than the other at similar levels of precision.

The second experiment is to implement the Smart Contracts and measure the data. Figure 7 shows Ethereum Gas consumption when adding new regions to the Smart Contracts. Gas is a term used in Ethereum that is equivalent to the computational energy consumption when executing a method in the Smart Contracts. The results showed that the gas consumption was irrelevant regardless of the level of precision and the geocoding technique used. The reason could be, as in the first experiment, that the characteristics of the polygon might affect the advantages of covering areas in each geocoding technique.

However, on giving a geocoded cell ID to query for the corresponding region, the results of the query time are those shown in Figure 8. From the result, it can be observed that Geohash is slightly faster than S2. The reason could be that

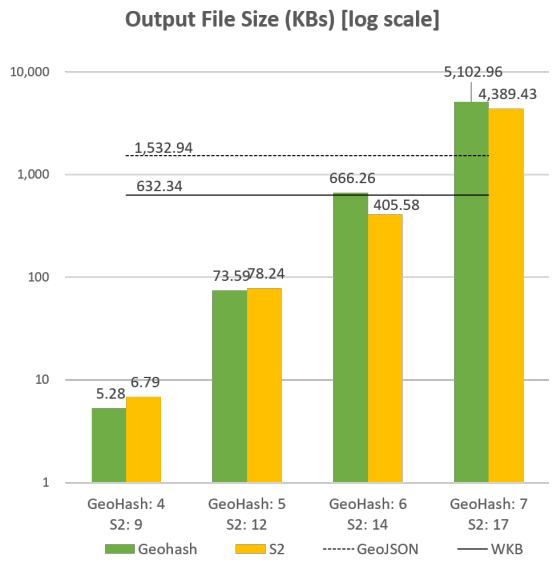

Fig. 6. File size comparison of geocoded polygons in Geohash and S2

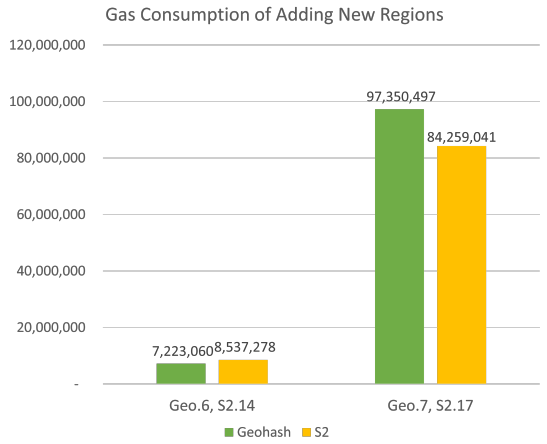

Fig. 7. Comparison of Ethereum gas consumption when adding geocoded cells to the Smart Contracts based on Geohash and S2

to iterate across the different levels of precision in the same geocoded cell, Geohash uses five bits to represent one level, while S2 uses two bits, which causes Geohash to iterate in a smaller number of loops.

VI. Conclusion

This work shows an architecture for managing end device reputation values in an IoT system, based on device geographical location. It splits the system into three layers: cloud, fog and edge layer. While end devices are in the edge layer, the reputation management system is located in the fog layer and operates in a decentralised way across different nodes in the layer using the Smart Contracts in the Ethereum Blockchain network. The management system divides an area into different regions, each of which contains a different reputation value for each device. The geospatial data associated with these

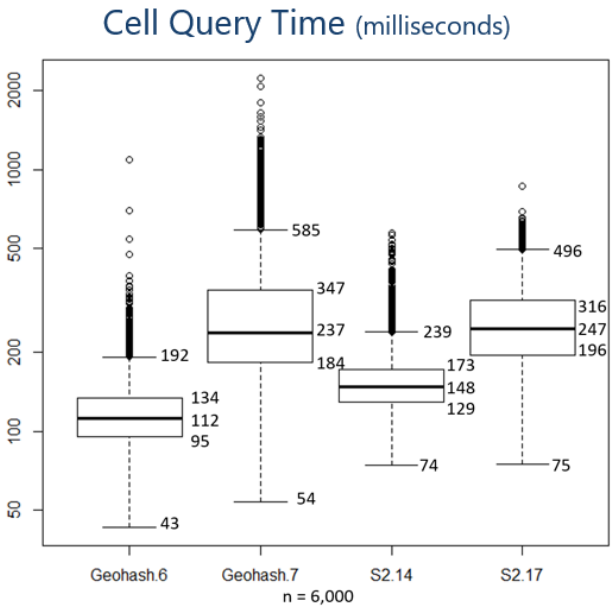

Fig. 8. Comparison of times to query for the destination region by giving a cell ID from Geohash or S2

regions are geocoded using hierarchical geocoding techniques (either Geohash or S2) to reduce complexity in the spatial calculation.

The first experiment compared the Geohash and S2 geocoding techniques in the context outside the Smart Contracts, by comparing the size and the time they needed to encode polygons into geocoded cells. The result showed that the output sizes were not different. The second experiment implemented the architecture, and ran it on simulated data. Using test polygons, the results showed that the amount of Ethereum gas consumed by Geohash and S2 was proportional to the input size, when they add these cells to the contracts. The results also demonstrated that Geohash is slightly faster than S2 when querying for a cell because it iterates less than Geohash to travel through all the levels.

This work has shown that the geospatial component can be included in the Smart Contracts, but there are still a few aspects that need to be improved and studied in greater depth in the future. The geocoded information in the Smart Contracts is currently used only to query whether the desired cell is inside the target region or not. However, future work could expand this part to perform another spatial calculation based on the same geocoded data: proximity calculation or area adjacency, for instance. Moreover, future research can also focus on reducing the data size to improve the performance, because a region consists of a set of geocoded cells that tend to have a mutual prefix with the other nearby cells.

REFERENCES

[1] Trilles, S., Calia, A., Belmonte, Ó., Torres-Sospedra, J., Montoliu, R., & Huerta, J. (2017). Deployment of an open sensorized platform in a smart city context. Future Generation Computer Systems, 76, 221-233.

[2] Trilles, S., Luján, A., Belmonte, Ó., Montoliu, R., Torres-Sospedra, J., & Huerta, J. (2015). SEnviro: A sensorized platform proposal using open hardware and open standards. Sensors, 15(3), 5555-5582.

[3] Atzori, L., Iera, A., and Morabito, G. (2011). Siot: Giving a social structure to the internet of things. IEEE Communications Letters, 15(11):1193=1195.

[4] Mui, L., Mohtashemi, M., and Halberstadt, A. (2002). A computational model of trust and reputation. In Proceedings of the 35th Annual Hawaii International Conference on System Sciences, pages 2431-2439

[5] Lenzini, G., Bargh, M. S., and Hulsebosch, B. (2008). Trust-enhanced security in location-based adaptive authentication. Electronic Notes in Theoretical Computer Science, 197(2):105-119. Proceedings of the 3rd International Workshop on Security and Trust Management (STM 2007).

[6] Golosova, J. and Romanovs, A. (2018). The advantages and disadvantages of the blockchain technology. In 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), pages 1-6.

[7] Atzori, L., Iera, A., Morabito, G., and Nitti, M. (2012). The social internet of things (siot) - when social networks meet the internet of things: Concept, architecture and network characterization. Computer Networks, 56(16):3594-3608.

[8] Artz, D. and Gil, Y. (2007). A survey of trust in computer science and the semantic web. Journal of Web Semantics, 5(2):58-71. Software Engineering and the Semantic Web.

[9] Cisco (2015). Unleash the power of the internet of things. Cisco Systems Inc.

[10] Trilles, S., Torres-Sospedra, J., Belmonte, Ó., Zarazaga-Soria, F. J., González-Pérez, A., & Huerta, J. (2020). Development of an open sensorized platform in a smart agriculture context: A vineyard support system for monitoring mildew disease. Sustainable Computing: Informatics and Systems, 28, 100309.

[11] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Satoshi Nakamoto Institute.

[12] Suwardi, I. S., Dharma, D., Satya, D. P., and Lestari, D. P. (2015). Geohash index based spatial data model for corporate. In 2015 International Conference on Electrical Engineering and Informatics (ICEEI), pages 478-483.

[13] Victor, F. and Zickau, S. (2018). Geofences on the blockchain: Enabling decentralized location-based services. In 2018 IEEE International Conference on Data Mining Workshops (ICDMW), pages 97-104.

[14] Chen, J., Tian, Z., Cui, X., Yin, L., and Wang, X. (2019). Trust architecture and reputation evaluation for internet of things. Journal of Ambient Intelligence and Humanized Computing, 10(8):3099-3107.

[15] Guo, J., Chen, I.-R., Wang, D.-C., Tsai, J. J. P., and Al-Hamadi, H. (2019). Trustbased iot cloud participatory sensing of air quality. Wireless Personal Communications, 105(4):1461-1474.

[16] Kouicem, D. E., Bouabdallah, A., and Lakhlef, H. (2018). An efficient architecture for trust management in ioe based systems of systems. In 2018 13th Annual Conference on System of Systems Engineering (SoSE), pages 138-143.

[17] Debe, M., Salah, K., Rehman, M. H. U., and Svetinovic, D. (2019). Iot public fog nodes reputation system: A decentralized solution using ethereum blockchain. IEEE Access, 7:178082-178093.

[18] Huh, S., Cho, S., and Kim, S. (2017). Managing iot devices using blockchain platform. In 2017 19th International Conference on Advanced Communication Technology (ICACT), pages 464-467.

[19] Fernando, E., Meyliana, and Surjandy (2019). Blockchain technology implementation in raspberry pi for private network. In 2019 International Conference on Sustainable Information Engineering and Technology (SIET), pages 154-158.

[20] Deiotte, R. and Valley, R. L. (2017). Comparison of spatiotemporal mapping techniques for enormous etl and exploitation patterns. ISPRS Annals of Photogrammetry, Remote Sensing & Spatial Information Sciences, 4.

[21] Miller, H. J. (1996). GIS and geometric representation in facility location problems. International Journal of Geographical Information Systems, 10(7), 791-816.